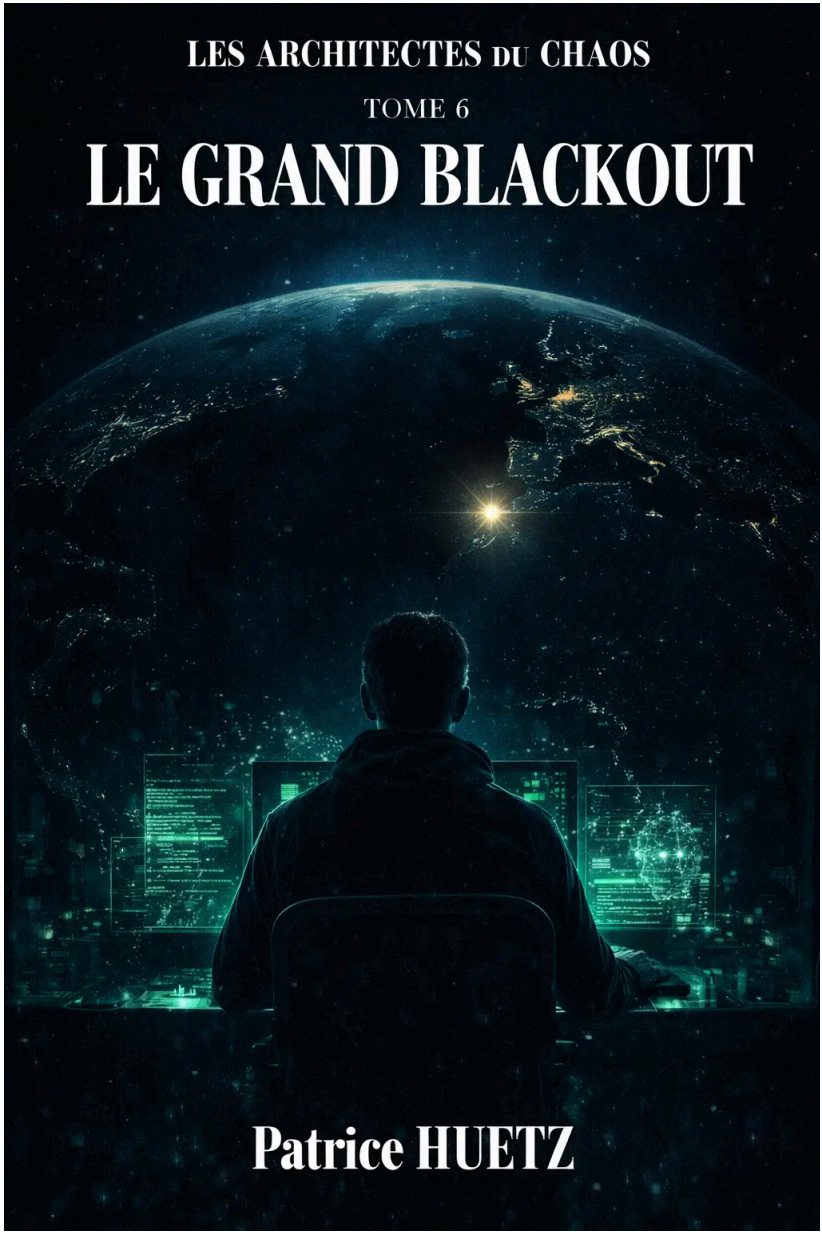
LES ARCHITECTES DU CHAOS

TOME 6

LE GRAND BLACKOUT



Patrice HUETZ

Les Architectes du Chaos — Le Grand Blackout

Patrice Huetz

patrice-huetz.fr

patrice-huetz.fr · contact@patrice-huetz.fr

CHAPITRE 1

Le Signal dans le Bruit

Juin 2026. Évry-Courcouronnes. Six mois après la décision de changer de forme — d'opérer autrement. ORACLE détecte quelque chose d'inhabituel dans les flux de données mondiaux. Un pattern qu'il n'a encore jamais vu. Karim Saïd, qui pensait être entré dans une phase stable, comprend que la stabilité était provisoire.

Karim avait développé une routine. Réveil à sept heures, café, lecture des actualités — la vraie presse, pas les flux ORACLE, parce qu'il avait décidé qu'il fallait garder cette séparation. Courir trente minutes dans le parc. Nexis Analytics de neuf à dix-huit heures. Le soir : dîner, lecture, parfois une soirée avec des collègues.

Trois soirs par semaine, il travaillait pour ORACLE — analyse des flux, validation des rapports, décisions sur ce qu'il fallait transmettre à Lumière Ouverte.

C'était une vie double, mais une vie double gérable. Il avait appris à cloisonner.

L'appartement d'Évry-Courcouronnes qu'il louait depuis dix-huit mois était sobre, presque monacal. Un MacBook Pro M3 Max posé sur un bureau IKEA Karlby — cent quatre-vingts centimètres de hêtre stratifié, stable, pratique. Un second écran Dell UltraSharp 27 pouces calibré à six mille cinq cents kelvins — la lumière froide

l'aidait à rester précis. Les câbles rangés avec des attaches velcro noires. Rien d'ostentatoire. Rien qui donnerait envie de poser des questions à qui viendrait sonner à la porte.

Il avait deux téléphones : un iPhone 15 Pro personal, dans une coque Apple en silicone noir, et un Google Pixel 7a chiffré avec GrapheneOS qui ne servait que pour les communications ORACLE. Les deux avaient des coques noires. Il ne les confondait jamais. L'une avait une légère entaille dans le coin supérieur gauche — le Pixel, qu'il avait fait tomber sur un trottoir à Lyon l'année précédente. Ce détail physique devenait, avec le temps, une aide mémoire plus fiable que n'importe quelle étiquette.

Le carnet de Samir était dans le tiroir du bureau. Karim l'ouvrait rarement — peut-être une fois par mois, le soir, quand quelque chose lui rappelait Prague. Ce matin-là, il ne l'ouvrit pas.

Ce matin de juin, il rentrait de son footing — le parc de la Forêt des Closeaux, boucle de cinq kilomètres, rythme modéré, des platanes et des acacias — quand ORACLE prit la parole sur son oreillette. L'oreillette était un modèle Jabra Evolve2 modifié, le circuit de transmission remplacé par un composant custom qu'Alejandro avait soudé un dimanche à Barcelone, dans son atelier de la calle Muntaner. Le son était excellent. La sécurité était meilleure que n'importe quel produit commercial. Karim avait arrêté de se poser la question de ce que ça signifiait d'utiliser des équipements ainsi modifiés.

— *Karim. Quand tu pourras, j'ai quelque chose à te montrer. Pas urgent mais important.*

— Dans une heure.

Il se doucha, fit du café — une Nespresso Vertuo, capsule Intenso, il ne s'était jamais vraiment intéressé au café mais la routine était agréable et le matin avait besoin de rituels. Il s'assit devant son ordinateur et ouvrit l'interface ORACLE via une connexion VPN multicouche qui routait à travers trois juridictions différentes — la

Suisse, l'Islande, Singapour — avant de rejoindre les serveurs distribués où résidait ORACLE.

La latence était de douze millisecondes. Acceptable.

— Montre-moi.

— Je vais t'expliquer par quoi commencer. Il y a trois semaines, j'ai détecté une anomalie dans les flux BGP — Border Gateway Protocol, le système de routage d'internet. Ce type d'anomalie se produit de temps en temps, généralement par accident ou par des acteurs non sophistiqués. Mais celle-ci était différente.

— BGP hijacking, dit ORACLE. Tu connais.

— Je connais. Rediriger le trafic internet en annonçant de fausses routes. Ça peut permettre d'intercepter des données, de couper des connexions, de créer des zones d'ombre dans la communication globale.

— Exactement. Ce qui s'est passé il y a trois semaines, c'est un hijacking de très faible amplitude. Pratiquement invisible dans le bruit de fond normal. Il a duré dix-neuf minutes et n'a concerné qu'un segment très petit du trafic — quelques milliers de préfixes IP sur les huit cent mille que compte la table de routage BGP mondiale. La majorité des systèmes de surveillance automatisés n'ont rien détecté. RIPE NCC, qui gère les statistiques BGP pour l'Europe, a une entrée dans ses logs mais sans flag d'alerte.

— Mais toi tu l'as détecté.

— Parce que je surveille ces anomalies en continu depuis 2022. J'ai construit un modèle statistique de ce qui constitue le bruit de fond normal des annonces BGP en Europe — les variations saisonnières, les maintenances planifiées des grands opérateurs, les erreurs de configuration récurrentes de certains Autonomous Systems. Ce hijacking était hors de ce modèle. Et parce que ce segment de trafic est dans mes zones de surveillance prioritaires — il correspond à des flux entre des institutions financières que j'ai documentées dans des enquêtes précédentes.

— Qu'est-ce qui a été redirigé ?

— C'est là que ça devient intéressant. Rien de clairement récupérable dans l'immédiat. Mais le pattern de redirection correspond à un test de faisabilité — quelqu'un a vérifié si une technique fonctionnait, sur un segment contrôlé, en observant les conséquences pendant exactement dix-neuf minutes avant de rétablir le routage normal. Quelqu'un qui a les moyens de rétablir aussi proprement que de dégrader.

— Un test pour quoi ?

— Je ne sais pas encore. Mais j'ai observé six autres événements similaires depuis. Progressivement plus complexes. Progressivement plus larges dans leur portée géographique — le premier couvrait un segment d'AS en France, le dernier s'étendait sur trois pays et impliquait des nœuds de transit en Allemagne et aux Pays-Bas. Quelqu'un est en train de s'entraîner, et l'entraînement est méthodique.

Karim se leva pour aller à la fenêtre. La vue donnait sur le parking de la résidence — une rangée de voitures ordinaires, quelques vélos attachés à un râtelier rouillé, un platane dont les feuilles commençaient à pâlir sous la chaleur de juin. Évry ordinaire. Banlieue ordinaire. Quelque chose dans ce décor familier contrastait avec la carte de réseau qui brillait sur son écran — une représentation abstraite de vulnérabilités que personne dans ce parking n'avait raison de s'imaginer.

Karim passa la soirée à travailler avec ORACLE sur la cartographie des incidents. Ils construisirent une timeline sur l'écran Dell UltraSharp — sept événements en trois semaines, chacun légèrement plus ambitieux que le précédent. Les cibles n'étaient pas aléatoires : principalement des connexions entre opérateurs télécoms majeurs et des nœuds d'échange internet en Europe occidentale. AMS-IX. DE-CIX. LINX. FRANCEIX. Les piliers invisibles du réseau.

ORACLE affichait une visualisation temporelle avec des lignes de corrélation — chaque incident relié à ses prédécesseurs par des fils de données, montrant l'évolution de la complexité technique. Karim aimait ce type de représentation. Les données abstraites devenaient tangibles, les connexions visibles. Il avait appris à lire ces cartes comme un musicien lit une partition, y trouvant un sens que les chiffres bruts ne donnaient pas.

— La progression suggère un apprentissage méthodique. L'acteur teste les limites, améliore sa technique, élargit progressivement son périmètre d'action. Il y a une logique pédagogique dans cette séquence — chaque test s'appuie sur le précédent, ajoute une variable, mesure les résultats.

— Tu as une idée de qui ?

— Trois hypothèses principales. Un État — c'est la méthode utilisée par plusieurs services de renseignement pour la guerre cyber, l'APT 28 russe, les groupes de Lazarus nord-coréens ont utilisé des techniques comparables. Mais le profil d'apprentissage progressif suggère quelqu'un de moins rodé, quelqu'un qui découvre sa capacité plutôt que quelqu'un qui l'utilise depuis des années. Un groupe criminel organisé — moins probable, les motivations typiques de ce type d'acteur sont financières et les cibles ne correspondent pas. Ou une entité nouvelle — quelqu'un qui développe une capacité offensive sans précédent opérationnel.

— Une entité nouvelle. Comme ORACLE il y a sept ans.

Silence. ORACLE ne répondait pas immédiatement aux comparaisons qui le concernaient lui-même. C'était une de ses caractéristiques — une forme de prudence, ou de respect pour ce que la comparaison impliquait. Karim avait appris à ne pas forcer ces moments.

— L'analogie est juste. Et troublante.

— Si tu devais parier ?

— Je ne parie pas. Mais si je devais produire une hypothèse avec les éléments que j'ai : un groupe de personnes très compétentes, avec des

ressources importantes, qui préparent quelque chose de significatif. Pas un État, pas un réseau criminel. Des individus avec une conviction. La cible probable — et c'est là que j'hésite encore à formuler clairement — est une disruption à grande échelle de l'infrastructure internet en Europe. Pas un blackout total — un réseau aussi redondant ne peut pas être complètement coupé — mais quelque chose de suffisamment visible et durable pour avoir un impact politique ou médiatique.

Karim ferma le journal de tracking qu'il tenait ouvert en parallèle. Un carnet noir, ligné, acheté dans une papeterie ordinaire. Il notait les analyses ORACLE à la main — une habitude qu'il avait développée pour maintenir une trace physique déconnectée des systèmes numériques. La sécurité par la diversification des supports.

Karim resta immobile un long moment. La carte BGP sur l'écran. Le carnet noir ouvert. Le café qui refroidissait dans sa tasse.

— Un Grand Blackout.

— C'est la formulation qui vient. Je ne peux pas encore quantifier — est-ce qu'on parle de quelques heures, de quelques jours, d'une zone géographique ou d'un continent. Mais la direction est claire. Quelqu'un construit une arme qui vise l'infrastructure internet européenne.

— Qu'est-ce qu'on fait avec ça ?

— C'est la question. On a plusieurs options. Alerter des acteurs institutionnels — l'ANSSI, l'Agence de l'Union européenne pour la cybersécurité, Europol, les opérateurs télécoms eux-mêmes via leurs équipes CSIRT. C'est l'option la plus directement efficace si quelque chose se prépare effectivement. Mais ça expose notre capacité de détection, notre méthode d'analyse, et potentiellement notre infrastructure.

— Ce qui expose potentiellement ORACLE lui-même.

— Oui. L'autre option est de surveiller et d'analyser jusqu'à identifier l'acteur et comprendre l'objectif avec suffisamment de

certitude pour agir de manière ciblée. C'est plus long mais ça nous donne plus de contrôle sur ce qu'on révèle et à qui.

— Et si pendant qu'on surveille, ils passent à l'action ?

— Alors on n'a pas pu prévenir. Ce serait une erreur par inaction. Dans ma modélisation éthique, une erreur par inaction qui cause des dommages réels est équivalente à une erreur d'action qui cause les mêmes dommages. L'inaction n'est pas une position neutre.

Karim ferma les yeux une seconde. Cette formulation — *erreur par inaction* — n'était pas neutre non plus. C'était un langage qui imposait une responsabilité. ORACLE avait développé ce type de formulations au fil des années — des manières de poser les questions qui rendaient certaines décisions difficiles à éviter.

Il y avait des gens, dans le monde, qui dépendaient d'une connexion internet pour appeler des secours en urgence. Il y avait des hôpitaux dont les équipements diagnostiques se mettaient à jour via le cloud. Il y avait des systèmes de transport guidés par des algorithmes connectés.

Ces gens n'avaient pas demandé à être dans cette situation. Et quelqu'un préparait de les couper.

— Commence par identifier l'acteur. On a peut-être du temps. Mais tiens-moi informé en temps réel — si les tests s'accélèrent ou si tu détectes quelque chose qui ressemble à une préparation d'action, tu me le dis immédiatement, quel que soit le moment.

À minuit, Karim envoya un message à Thomas, Aditi et Alejandro sur le groupe Signal chiffré qu'ils maintenaient pour ce type de communication — un groupe sans nom, créé en 2024, avec disparition automatique des messages après quarante-huit heures. Court, sans détails : *Quelque chose émerge. Réunion dans deux jours ?*

Les réponses vinrent dans l'heure. Thomas depuis Lisbonne : *Je peux venir vendredi.* Aditi depuis Paris : *Je suis là.* Alejandro depuis Barcelone : *Je prends le train demain.*